RMT/JN/DG
F.#2012R00103

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF AN APPLE IPAD, SERIAL NUMBER DLXG6RDHDFJ3, CURRENTLY LOCATED IN THE CUSTODY OF THE FEDERAL BUREAU OF INVESTIGATION	APPLICATION FOR A SEARCH WARRANT FOR AN ELECTRONIC DEVICE Case No. MISC 18 - 1320

DEARIE, J.

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jonathan Polonitza, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 1(c) of the Federal Rules of Criminal Procedure, Rule 41 of the Federal Rules of Criminal Procedure, the inherent authority of the district court to issue warrants under Article III of the United States Constitution, and the Fourth Amendment to the United States Constitution,[1] for a search warrant authorizing the examination of an electronic device currently in law enforcement

---

[1] In United States v. Villegas, 899 F.2d 1324, 1334 (2d Cir. 1990), the Court of Appeals for the Second Circuit stated that "Rule 41 does not define the extent of the court's power to issue a search warrant," and "[o]bviously, the Fourth Amendment long antedated the Federal Rules of Criminal Procedure, which were first adopted in 1944." The Second Circuit further recognized that: "[g]iven the Fourth Amendment's warrant requirements, and assuming no statutory prohibitions, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met." Id. (internal citations omitted).

custody, more particularly described in Attachment A, and the extraction from that device of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since January 2011. I am responsible for conducting and assisting in investigations into the activities of individuals and criminal groups responsible for crimes related to the unlawful accessing and use of computer media. I am one of the case agents with primary responsibility for this investigation. While working for the FBI, I have participated in numerous investigations of criminal activity, including bank fraud, securities fraud, corporate fraud, insider trading, money laundering schemes and other types of schemes. During the course of these investigations, I have conducted or participated in surveillance, undercover transactions, the execution of search warrants, debriefings of informants and reviews of taped conversations and financial records. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is an Apple iPad, serial number DLXG6RDHDFJ3, hereinafter the "Device." The Device is currently in the possession of the FBI at 26 Federal Plaza, New York, New York.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. In or about and between February 2010 and August 2015, Vitaly Korchevsky, together with others (collectively, the "Subject Individuals"), engaged in a scheme whereby they executed and caused others to execute securities transactions in certain publicly traded companies (the "Target Companies") based in whole or in part on material, nonpublic information ("MNPI") that was fraudulently obtained through unauthorized attacks on the computer networks of PR Newswire Association LLC ("PR Newswire"), Marketwired L.P. ("Marketwired") and Business Wire (collectively, the "Victim Newswires") that were in the business of disseminating press releases for corporate clients. The Subject Individuals stole MNPI about the Target Companies, which was in the form of confidential press releases, by using sophisticated computer intrusion techniques, such as SQL injection and brute force attacks, and then traded in the Target Companies' securities based on the stolen MNPI for substantial financial gain.

7. The Subject Individuals were generally organized into three groups: (i) the individuals who used sophisticated intrusion techniques and stole MNPI from the Victim Newswires' computer networks from overseas locations such as Ukraine and Russia (collectively, the "Hackers"); (ii) the individuals who executed securities transactions based on the stolen MNPI, including Vitaly Korchevsky (collectively, the "Traders"); and (iii) the

individuals who communicated and coordinated between the Hackers and Traders (collectively, the "Middlemen").

8. The MNPI stolen by the Hackers contained information relating to the Target Companies' earnings, gross margins, revenues and other confidential and material financial information. Thus, the confidential press releases contained economically valuable information and the Victim Newswires and Target Companies had a right to control the use of that information. The Target Companies provided the Victim Newswires with this MNPI, typically in press releases, which was then uploaded on the Victim Newswires' computer networks and disseminated to the public at the direction of the Target Companies. Until the contracted distribution time, the Victim Newswires were contractually bound to keep the content of the press releases confidential and non-public.

9. The Target Companies' press releases were maintained on the Victim Newswires' computer networks for a limited period of time. Consequently, the Hackers had to steal the MNPI shortly after it was uploaded onto the Victim Newswires' computer networks and transmit the MNPI to the Traders through the Middlemen so that the Traders could engage in illegal securities transactions before the MNPI was released to the public (hereinafter referred to as "inside-the-window" trades). This investigation has revealed numerous instances where the Traders engaged in such inside-the-window transactions at times where it was subsequently determined through forensic analysis that the Victim Newswires' computer networks had been compromised through hacking. Therefore, and based on evidence of efforts by the Traders to transfer portions of the illegally obtained proceeds of the fraudulent trading to certain Hackers (as described further below), there is

reason to believe that the Hackers, Middlemen and Traders were conspiring together in furtherance of this fraudulent scheme.

10. In sum, in or about and between January 2011 and May 2015, the Subject Individuals stole approximately 100,000 press releases and executed at least 1,000 inside-the-window trades in the Target Companies based on MNPI stolen from the Victim Newswires resulting in more than $30 million in illegal profits.

11. On August 5, 2015, a grand jury in the Eastern District of New York returned an indictment charging Korchevsky and others with (1) conspiring to commit wire fraud, in violation of Title 18, United States Code, Section 1349; (2) conspiring to commit securities fraud, in violation of Title 18, United States Code, Section 371; (3) securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff; and (4) conspiring to commit money laundering, in violation of Title 18, United States Code, Section 1956(h). See 15-CR-381 (RJD). A warrant was issued for his arrest that same day.

12. On August 11, 2015, Korchevsky was arrested at his home in Glen Mills, Pennsylvania. On that same date, FBI agents executed a search warrant at his residence, a copy of which is attached to this application as Exhibit A. That search warrant authorized the seizure of, inter alia, "[c]omputer hardware consist[ing] of all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic optical, or similar computer impulses or data." (See VK-000055705). It further authorized the seizure of data from such computers that was evidence of violations of 18 U.S.C. §§ 371, 1030(a)(2), 1349 and 1956(h). (See VK000055707-09).

13. Among the materials seized from Korchevsky's home pursuant to the above-referenced search warrant was the Device. Also pursuant to the search warrant, FBI examiners conducted a forensic review of the Device, ultimately producing a forensic image report dated October 2, 2015 that was subsequent produced to Korchevsky and his-co-defendant pursuant to the government's Rule 16 obligations.

14. During subsequent debriefings with certain of Korchevsky's co-conspirators, those individuals told agents that the conspiracy employed numerous overseas email accounts to allow the Hackers to transmit stolen press releases to the Traders.

15. Korchevsky's trial is scheduled to commence on June 11, 2018. In the course of preparing exhibits for trial, I and other trial team members have reviewed emails of co-conspirators. We identified an email sent on or about May 15, 2012 in which one co-conspirator sent another Trader in the scheme the email address "stargate11@e-mail.ua" (the "Stargate Email Address"), along with login credentials for that account. Based on my training and experience, I know that ".ua" indicates a Ukraine-based Internet domain.

16. In reviewing the forensic report for the Device, I have observed indications that the Device accessed the Stargate Email Address and downloaded at least four emails on or about July 30, 2012. The body of these emails contains the word "Updates," and the emails appear to have attachments. Based on my knowledge of the investigation, there is probable cause to believe those attachments are stolen press releases. However, the forensic image originally taken of the Device did not successfully extract those attachments.

17. I have been advised by an FBI forensic examiner that the FBI forensic lab in Quantico, Virginia has specialized capabilities that may allow technicians there to further examine the Device, access those and any other emails associated with the Stargate Email Address, and extract all data associated with them, including any email attachments.

18. For these reasons, while the FBI may already have all necessary authority to examine the Device based on the prior search warrant, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device by forensic examiners at the FBI laboratory in Quantico, Virginia will comply with the Fourth Amendment and other applicable laws.

19. The Device is currently in storage at 26 Federal Plaza. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the Federal Bureau of Investigation in August 2015.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the inherent authority of the district court to issue warrants under Article III of the United States Constitution, and the Fourth Amendment to the United States Constitution the warrant I am applying for would permit the examination of the device consistent with the warrant, including examination outside the Eastern District of New York. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

24. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Jonathan Polonitza
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on May 10, 2018:

THE HON. RAYMOND J. DEARIE
SENIOR UNITED STATES DISTRICT JUDGE

ATTACHMENT A

The property to be searched is an Apple iPad, serial number DLXG6RDHDFJ3, hereinafter the "Device." The Device is currently in the possession of the Federal Bureau of Investigation at 26 Federal Plaza, New York, New York.

This warrant authorizes the forensic examination of the Device for the purpose of identifying and extracting the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A associated with the email address stargate11@e-mail.ua that relate to violations of 18 U.S.C. §§ 371, 1030(a)(2), 1349 and 1956(h) and involve Vitaly Korchevsky since February 1, 2010, including the contents of those emails, and associated attachments; and

2. Evidence of user attribution showing who used the Device at the times the stargate11@e-mail.ua was accessed, since February 1, 2010.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.